ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

Security Scheme in Cloud Computing

Prof. Rajesh V[1], Dr.K S Jagadeesh Gowda[2], Prof. AnandaPadmanabha. R[3]

Assistant Professor, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Bengaluru, India

Professor & HOD, Department of Computer Science and Engineering, Sri Krishna Institute of Technology, Chikkabanavara, Bangalore, India

Research associate, Department of Computer Science and Engineering, B.M.S. Institute of Technology, Bengaluru, India

ABSTRACT*:* With searchable encryption, a data user is able to perform meaningful search on encrypted data stored in the public cloud without revealing data privacy.One of the most favoured encryption innovations to tackle the testing issue of secure information partaking in distributed computing is Ciphertext-policy attribute-based encryption (CP-ABE). A productive record chain of importance attribute-based encryption plan is proposed in distributed computing.First, we provide an overview of the state of the art on cloud security. Then, we introduce the notion of cloud security assurance and analyze its growing impact on cloud security approaches.The ciphertext parts identified with attributes could be shared by the records. Accordingly, both ciphertext data storage and time cost of encryption are bifurcated. In addition, the proposed plan is ended up being secure under the standard presumption. Test re-enactment demonstrates that the proposed plan is very proficient regarding encryption and decryption. With the quantity of the records expanding, the upsides of our plan turn out to be increasingly prominent.

KEYWORDS: Ciphertext-policy, attribute-based encryption, data sharing, file hierarchy.

I. INTRODUCTION

Attributes define, classify, or annotate the datum to which they are assigned. As a significant research area for system protection, data access control has been evolving in the past thirty years and various techniques [6]–[9] have been developed to effectively implement fine-grained access control, which allows flexibility in specifying differential access rights of individual users. For the purpose of helping the data owner enjoy fine-grained access control of data stored on untrusted cloud servers, a feasible solution would be encrypting data through certain cryptographic primitive(s), and disclosing decryption keys only to authorized users. Unauthorized users, including cloud servers, are not able to decrypt since they do not have the data decryption keys. Ciphertext-policy attribute based encryption (CP-ABE) [2] is a public-key cryptography primitive that was proposed to resolve the exact issue of fine-grained access control on shared data in one-to-many communications. In the last few years, the security research community has worked hard to improve the security of the cloud infrastructure and the trust of cloud users that their applications and information are correctly managed and protected.

II. LITERATURE SURVEY

[1]THE AUTHOR,Jia W, Zhu H (ET .AL), AIM we project a secure mobile user-based data service mechanism (SDSM) to give secrecy and fine-grained get to control for information put away in the cloud. This system empowers the versatile clients to appreciate safe outsourced information administrations at a limited security administration overhead. The core thought of SDSM is that SDSM outsources the information as well as the security administration to the portable cloud in a trust way. Our investigation demonstrates that the proposed instrument has many focal points

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology
An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018
2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"
13th-14th March 2018
Organized by
Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

over the current conventional strategies; for example, bring down overhead and advantageous refresh, which could better cook the necessities in versatile distributed computing situations.

[2]THE AUTHOR, Zhou Z, (ET .AL), AIM weshow a far reaching security information request system for portable distributed computing. Our answer concentrates on the accompanying two research headings: First, we present a novel Privacy Preserving Cipher Policy Attribute-Based Encryption (PP-CP-ABE) to protect sensing data. Using PP-CP-ABE, light-weight devices can securely outsource heavy encryption and decryption operations to cloud service providers, without revealing the data content. Second, we propose an Attribute Based Data Storage (ABDS) system as a cryptographic group-based access control mechanism.

[3] Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. Authors: Cong Wang, KuiRen, And Shucheng Yu Description: In this paper, It investigate the problem of secure and efficient similarity search over outsourced cloud data. In this any user can upload data on cloud and also achieves the usable and privacy assured similarity search over outsourced cloud data.

[4] Hybrid attribute- and re-encryption-based key management for secure and scalable mobile applications in clouds. Authors: P. K. Tysowski and M. A.HasanDescription: cloud-based data are increasingly accessed by resource-constrained mobile devices for which the processing cost must be minimized. In this paper, re-encryption mechanism is performed optionally.

III. METHODS AND TECNIQUES USED

ATTRIBUTEBASED ENCRYPTION

We now give an overview of Attribute-Based Encryption (ABE) algorithms. The Sahai-Waters (ABE) cryptosystem as implemented in this paper is specifically detailed. We focus our efforts on providing the description of the scheme and intuition for its construction. For the proof of security see Sahai and Waters. Attribute-Based Encryption can be viewed as a generalization of Identity-Based Encryption (IBE) [5]. A party in the system can encrypt a message to this particular user with only the knowledge of the recipient's identity and the system's public parameters. In particular the encryption algorithm does not need to have access to a separate public key certificate of the recipient. In Attribute-Based Encryption a user's identity is composed of a set, S, of strings which serve as descriptive attributes of the user. For example, a user's identity could consist of attributes describing their university, department, and job function. A party in the system can then specify another set of attributes S0such that a receiver can only decrypt a message if his identity S has at least k attributes in common with the set S0, where k is a parameter set by the system. Like traditional Identity-Based Encryption, a party in an Attribute-Based Encryption system only needs to know the receiver's description in order to determine their public key. However, the expressiveness of an ABE system is potentially much more powerful. For example, there could be several different recipients that are able to decrypt a message encrypted for a set S0.

SEMI-TRUSTED SERVER

LDSS is designed under the same assumptions proposed in 0 that the CSP is honest but curious, which means that the CSP will faithfully execute the operations requested by users, but it will peek on what users have stored in the cloud. The CSP will faithfully store users' data, undertake an initial access control, update data according to users' requests. However, CSP may do malicious actions such as collusion with users to get the data in plain text.In LDSS, proxy encryption server and proxy decryption server are introduced to assist users to encrypt and decrypt data so that user-side overhead can be minimized. In essence, proxy servers are also machines in the cloud. Thus, we consider that they are honest but curious just as the CSP.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization Volume 7, Special Issue 6, May 2018

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

TRUSTED AUTHORITY

In this paper, to make LDSS feasible in practice, a trusted authority (TA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user. The fact that a trusted channel exists doesn't mean that the data can be shared through the trusted channel, for the data can be in a large amount. TA is only used to transfer keys (in a small amount) securely between users. In addition, it's requested that TA is online all the time because data users may access data at any time and need TA to update attribute keys.

LAZY RE-ENCRYPTION

In ciphertext access control, data needs to be re-encrypted when some users' access privileges to the data are revoked. However, frequent re-encryption brings heavy computational overhead, and the accessed plaintext data may already be stored on these data users. Therefore, this paper adopts the lazy re-encryption method proposed in [3]. With lazy re-encryption, when a user's access privilege is revoked, data is not re-encrypted until the data owner updates the data.

APPLICATION OF POLICY

The threshold, conjunction and disjunction constructions discussed in Section 4 results in an expressive policy system. In this section we illustrate the use of policy in two separate applications: HIPAA compliant distributed storage systems and social networks.

DISTRIBUTED FILE SYSTEMS

A content-addressable file system enables users to locate files based on attributes or keywords describing their contents. Example systems include large multisite research efforts such as the Human Genome Project, which was formed in order to map the sequence of chemical building blocks composing the human genome. While this multinational research effort requires a total of only 3 gigabytes of space to store the genome itself, the space estimated for additional annotationswill sufficiently dwarf the initial sequence data in the system [1]. As this and other research projects begin to require petabytes of storage, the ability to securely store such information across multiple sites becomes increasingly critical. We use a Health Insurance Portability and Accountability Act (HIPAA) compliant medical system as an example of a loosely-coupled, content-addressable file system with strict security requirements. HIPAA was designed to clearly enumerate the security requirements and provide information flow control for electronically stored medical information such that patient privacy is maintained.

Iv. CONCLUSION

In this paper we addressed an important issue of attribute revocation for attribute based systems. In particular, we considered practical application scenarios in which semi-trustable proxy servers are available, and proposed a scheme supporting attribute revocation. One nice property of our proposed scheme is that it places minimal load on authority upon attribute revocation events. We achieved this by uniquely combining the proxy re-encryption technique with CP-ABE and enabled the authority to delegate most laborious tasks to proxy servers. Our proposed scheme is provably secure against chosen ciphertext attacks. In addition, we also showed the applicability of our method to the KP-ABE scheme. One interesting future work is to combine a secure computation technique with our construction to guarantee the honesty of proxy servers. Another direction for future work is to allow proxy servers to update user secret key without disclosing user attribute information.

ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

International Journal of Innovative Research in Science, Engineering and Technology

An ISO 3297: 2007 Certified Organization *Volume 7, Special Issue 6, May 2018*

2nd National Conference on "RECENT TRENDS IN COMPUTER SCIENCE & INFORMATION TECHNOLOGY (RTCSIT'18)"

13th-14th March 2018

Organized by

Departments of Computer Science & Information Science Engineering, Sri Krishna Institute of Technology, Bangalore, India

REFERENCES

[1] Fraudster. http://www.friendster.com, 2006.
[2] J. Bettencourt, A. Sahai, and B. Waters.Ciphertext-Policy Attribute-Based Encryption.InProc. of SP'07, Washington, DC, USA, 2007.
[3] Qihua Wang, HongxiaJin. "Data leakage mitigation for discretionary access control in collaboration clouds".The 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.
[4] Adam Skillen and Mohammad Mannan.On Implementing Deniable Storage Encryption for Mobile Devices.the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.
[5] D. Boneh and M. K. Franklin.Identity-based encryption from the Weil pairing. In Proceedings of the 21st Annual International Cryptology Conference on Advances in Cryptology, pages 213–229. Springer-Verlag, 2001.
[6] H. Harney, A. Colgrove, and P. D. McDaniel, "Principles of policy in secure groups," in Proc. of NDSS'01, 2001.
[7] Kan Yang, XiaohuaJia, KuiRen: Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIACCS 2013, pp. 523-528, 2013.
[8] Crampton J, Martin K, Wild P. On key assignment for hierarchical access control.in: Computer Security Foundations Workshop. IEEE press, pp. 14-111, 2006.
[9] J. Li, N. Li, and W. H. Winsborough, "Automated trust negotiation using cryptographic credentials," in Proc. of CCS'05, 2005.
[10] Cong Wang, KuiRen, Shucheng Yu, and KarthikMahendraRajeUrs.Achieving Usable and Privacy-assured Similarity Search over Outsourced Cloud Data. IEEE INFOCOM 2012, Orlando, Florida, March 25-30, 2012
11] Yu S., Wang C., Ren K., Lou W. Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing. INFOCOM 2010, pp. 534-542, 2010
[12] Kan Yang, XiaohuaJia, KuiRen, Bo Zhang, RuitaoXie: DACMACS: Effective Data Access Control for Multiauthority Cloud Storage Systems. IEEE Transactions on Information Forensics and Security, Vol. 8, No. 11, pp.1790-1801, 2013.
[13] Stehlé D, Steinfeld R. Faster fully homomorphic encryption. in: Proceedings of 16th International Conference on the Theory and Application of Cryptology and Information Security. Singapore: Springer press, pp.377-394, 2010.
[14] Junzuo Lai, Robert H. Deng ,Yingjiu Li ,et al. Fully secure key policy attribute-based encryption with constant-size ciphertexts and fast decryption. In: Proceedings of the 9th ACM symposium on Information, Computer and Communications Security (ASIACCS), pp. 239-248, Jun. 2014.
[15] Bethencourt J, Sahai A, Waters B. Ciphertext-policy attributeIEEE Transactions on Cloud Computing, January 2017 based encryption. in: Proceedings of the 2007 IEEE Symposium on Security and Privacy (SP). Washington, USA: IEEE Computer Society, pp. 321-334, 2007.

.

.